(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 820 847**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **01 01901**

(51) Int Cl[7] : G 06 F 12/14

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 12.02.01.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 16.08.02 Bulletin 02/33.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *GEMPLUS Société anonyme* — FR.

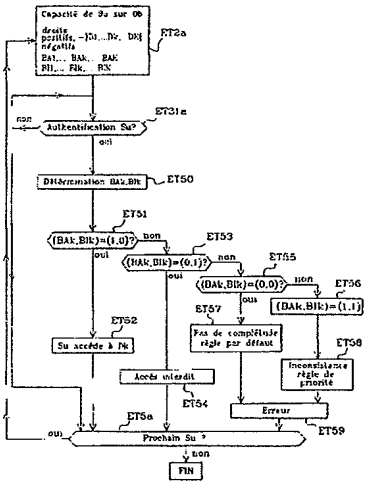
(72) Inventeur(s) : AMEGAH ANDRE et BIDAN CHRISTOPHE.

(73) Titulaire(s) :

(74) Mandataire(s) :

(54) CONTROLE D'ACCES DE SUJETS A DES OBJETS NOTAMMENT DANS UNE CARTE A MICROCONTROLEUR.

(57) L'invention concerne à la fois des listes de contrôles d'accès de sujets à des objets et des capacités d'actions de chaque sujet à un objet donné. Par exemple les sujets et les objets sont des utilisateurs et des applications dans une carte à puce. Des indicateurs (BAk, Blk) sont enregistrés dans la carte. Chaque indicateur a un premier état pour autoriser/ interdire l'accès de sujets à un objet et un deuxième état pour ne pas autoriser/ ne pas interdire l'accès des sujets aux objets. L'invention introduit ainsi des droits d'accès négatifs dans les listes de contrôle d'accès et les capacités.



FR 2 820 847 - A1

2820847

Contrôle d'accès de sujets à des objets notamment dans une carte à microcontrôleur

La présente invention concerne d'une manière générale le contrôle d'accès de premiers éléments, tels que des sujets constituant des "utilisateurs" d'un moyen de traitement de données ou bien des modules logiciels dans ce moyen de traitement de données, à des objets tels que des applications implémentées dans le moyen de traitement de données. Plus particulièrement, l'invention est relative au contrôle d'accès à des applications implémentées dans une carte à puce, dite également carte à microcontrôleur ou à circuit intégré, qui comporte plusieurs applications, proposant divers services à des utilisateurs, tels que des applications de commerce électronique, porte-monnaie électronique, services de fidélité, etc.

Du point de vue de la sécurité, la coexistence et la coopération de plusieurs applications au sein d'une même carte à puce soulève de nombreux problèmes. En particulier, chaque application possède ses propres données pour lesquelles ses propres droits d'accès sont définis. Ainsi, il est essentiel au sein de la carte à puce de mettre en oeuvre des moyens de sécurité pour contrôler l'accès aux données des applications depuis des accès externes, par exemple par les utilisateurs de la carte qui peuvent être des modules logiciels comme des interfaces d'usagers, mais également depuis des accès internes, par exemple par l'intermédiaire d'autres applications ou d'éléments logiciels d'application dans la carte.

Dans ce cadre du contrôle d'accès discrétionnaire, les sujets, tels que des

utilisateurs, sont des éléments "actifs" qui manipulent des informations contenues dans des objets, tels que des applications, qui sont des éléments "passifs" contenant des données. Les sujets ont leurs accès conditionnés par des droits d'accès sous la forme de règles de contrôle d'accès entre les sujets et les objets. Les sujets peuvent avoir la capacité de passer leurs droits d'accès à d'autres sujets, et pour chaque accès, les règles de contrôle doivent autoriser ou s'abstenir d'autoriser l'accès à des sujets déterminés.

L'état des autorisations d'accès à des objets dans un moyen de traitement de données, tel que la carte à puce, est exprimé généralement par une matrice d'accès MA dont les lignes correspondent à des sujets et dont les colonnes correspondent à des objets, comme montré à la figure 1. Par exemple, la matrice MA est relative à trois sujets S1, S2 et S3, tels que trois utilisateurs, et à quatre objets, tels que trois fichiers F1, F2 et F3 et un programme P1. Chaque case de la matrice à l'intersection d'une ligne et d'une colonne contient des droits définissant des actions privilégiées qui peuvent être accomplies par le sujet respectif sur l'objet respectif. Par exemple, ces actions peuvent être l'enregistrement d'un fichier ou d'un programme, ou bien la lecture ou l'écriture d'un fichier, ou bien la lecture, l'écriture ou l'exécution d'un programme.

Deux approches sont mises en oeuvre pour régir la matrice de contrôle d'accès.

La première approche consiste à mémoriser des indicateurs d'accès constitués par les droits d'accès colonne par colonne de la matrice de contrôle d'accès afin de constituer des listes de contrôle d'accès ACL (Access Control List) spécifiant chacune les droits

d'accès de sujets à l'objet associé à la colonne. A titre d'exemple, dans une carte à puce multi-applicative du type WINDOWS (marque enregistrée), des listes de contrôle d'accès ACL accordent des accès en lecture et/ou en écriture à des sujets, tels que des utilisateurs de la carte, sur des objets, tels que des fichiers, mais également permettent d'interdire l'accès par tous les sujets à un fichier constituant un objet.

Pour ce qui concerne chaque liste de contrôle d'accès ACL dans la matrice d'accès montrée à la figure 1, chaque sujet de la liste est authentifié et la liste des droits d'accès est analysée. La révocation et la révision des droits d'accès sont facilement exécutées pour coder des listes de droit d'accès.

La deuxième approche consiste à exprimer par des capacités regroupant des indicateurs d'accès correspondant à des droits d'accès ligne par ligne de la matrice de contrôle d'accès afin de définir pour chaque sujet les droits d'accès qu'il possède sur des objets. Par exemple, le contrôle d'accès porte sur des méthodes d'applets pour cartes à puce multi-applicatives de type JavaCard dans lesquelles des programmes ont été écrits en langage Java. Les capacités correspondent à des pointeurs effectuant des appels pour accéder à des méthodes constituant des objets, dans des applets prédéterminées constituant des sujets.

En ce qui concerne les capacités d'accès, chacune peut être exprimée par des couples d'indicateurs comprenant le nom d'un objet et d'un ensemble de privilèges ou droits. Cette capacité ainsi définie est mémorisée dans la carte. Une telle

capacité est complètement transférable d'un sujet à un autre.

Ainsi, actuellement, les droits d'accès sont toujours exprimés sous une forme positive. Tout droit d'accès non autorisé ne peut pas être exprimé pour un sujet particulier et ne peut pas être déduit de son absence dans une liste de droits d'accès autorisés.

Du point de vue de la sécurité, le fait de ne pas exprimer explicitement des accès interdit risque d'accorder, par erreur, un accès illicite à un sujet.

Les règles de contrôle d'accès selon la technique antérieure ne permettent d'exprimer que des droits d'accès positifs, c'est-à-dire des accès autorisés et ne permettent pas de garantir qu'un sujet donné ne possède pas un droit d'accès sur un objet donné, ou ne peut acquérir de manière indirecte le droit d'accès de par l'appartenance à un groupe qui possède ce droit d'accès.

Dans un contexte de définition de droits d'accès par l'approche de liste de contrôle d'accès, il est supposé que l'on veuille donner un accès sur un objet sensible à tous les sujets d'un groupe sauf un, noté S. En présence que de droits positifs, il faut énoncer explicitement l'accès pour chaque membre du groupe excepté le sujet S.

Selon un autre exemple, l'objet F1 représente une donnée sensible d'une application, telle qu'une clé de chiffrement, pour laquelle le sujet S1 a des droits de lecture, d'écriture et d'enregistrement exprimés sous forme de capacité. Le sujet S2 n'a aucun droit sur l'objet F1. Les droits d'accès positifs sont définis par des capacités respectivement associées aux sujets. Comme déjà dit,

une spécificité des capacités est la possibilité de transférer des droits d'accès d'un sujet à un autre. Toutefois, avec cette définition de droits d'accès positifs, il est impossible de vérifier qu'un sujet non autorisé à accéder à un objet donné ne peut acquérir la capacité permettant d'outrepasser cette interdiction. L'incohérence de droit d'accès à un même objet par un sujet n'est pas vérifiée. Ainsi, en présence que de droits positifs, il est complexe de s'assurer que le sujet S2 n'a pas accès à l'objet F1 après un transfert de capacité du sujet S1 vers le sujet S2.

D'une manière plus générale, lors de la définition ou la suppression ou la modification de droit d'accès ou de sujets se pose le problème de la cohérence de nouveaux droits d'accès vis à vis de droits préalables.

L'objectif principal de la présente invention est de remédier aux inconvénients de la définition des droits d'accès positifs selon la technique antérieure, de manière à spécifier explicitement des accès interdits à des objets par des sujets aussi bien dans les listes de contrôle d'accès que dans les capacités.

Pour atteindre cet objectif, un procédé pour contrôler des accès de premiers éléments à des deuxièmes éléments dans un moyen de traitement de données, est caractérisé par un enregistrement dans le moyen de traitement d'indicateurs d'autorisation ayant chacun un premier état pour autoriser explicitement un accès au moins d'un premier élément à un deuxième élément et un deuxième état pour ne pas autoriser ledit accès, et d'indicateurs

d'interdiction ayant le premier état pour interdire explicitement un accès au moins d'un premier élément à un deuxième élément et le deuxième état pour ne pas interdire ledit accès, l'accès étant autorisé ou interdit après une analyse conjointe des indicateurs d'autorisation et d'interdiction relatifs à l'accès.

Comme on le verra dans la suite, les premiers éléments sont par exemple des sujets tels que des utilisateurs, et les deuxièmes éléments sont par exemple des objets, tels que des applications, dans une carte à puce multi-applicative constituant le moyen de traitement de données.

En ce qui concerne les listes de contrôle d'accès, c'est-à-dire pour donner l'accès d'un premier élément parmi plusieurs premiers éléments d'un ensemble à un deuxième élément, le procédé comprend les étapes de :

- dresser une première liste de premiers éléments auquel l'accès au deuxième élément est autorisé et une deuxième liste de premiers éléments auquel l'accès aux deuxièmes éléments est interdit,
- mettre respectivement au premier état l'indicateur d'un premier élément des première et deuxième listes lorsque le premier élément est authentifié et au deuxième état lorsque le premier élément n'est pas authentifié,
- évaluer un indicateur d'autorisation en fonction des indicateurs des éléments dans la première liste et un indicateur d'interdiction en fonction des indicateurs des éléments dans la deuxième liste, et
- n'autoriser l'accès du premier élément au deuxième élément que lorsque les indicateurs d'autorisation et d'interdiction sont respectivement au premier état et au deuxième état, et n'interdire

l'accès du premier élément au deuxième élément que lorsque les indicateurs d'autorisation et d'interdiction sont respectivement au deuxième état et au premier état.

L'introduction de droit d'accès négatif dans les listes de contrôle d'accès selon l'invention permet de spécifier explicitement qu'un sujet donné n'est pas autorisé à accéder à un objet donné. Il devient ainsi aisé de garantir que le sujet ne peut accéder à l'objet. Les droits d'accès négatifs selon l'invention sont individuels contrairement à l'interdiction d'accès de tous les sujets à un objet selon la technique antérieure.

Lorsque les indicateurs d'autorisation et d'interdiction sont tous deux au deuxième état, l'accès peut être par défaut autorisé ou interdit. Dans ce cas, une erreur de complétude peut être signalée. A contrario, lorsque les indicateurs d'autorisation et d'interdiction sont tous deux au premier état, l'accès peut être par priorité autorisé ou interdit. Dans ce cas, une erreur de consistance peut être signalée.

L'invention reprend le concept de groupe de premier élément si bien que des groupes sont compris dans les première et deuxième listes. Chaque groupe est considéré comme authentifié lorsque l'un des éléments du groupe est authentifié. L'indicateur d'un groupe contenant un élément authentifié est alors mis au premier état avant d'évaluer les indicateurs des listes.

L'invention crée un concept d'association de premier élément. Dans ce cas, les première et deuxième listes comprennent des associations de premier élément auxquelles des indicateurs d'association correspondent pour autoriser ou

interdire l'accès de l'association au deuxième élément. Chaque association est considérée comme authentifiée lorsque tous les membres de l'association sont authentifiés. L'indicateur d'une association contenant un élément authentifié est mis égal au produit des indicateurs des membres de l'association avant d'évaluer les indicateurs des listes.

De préférence, au moins un membre dans une association dans l'une des deux listes est un groupe. Lorsque l'un des éléments du groupe est authentifié, l'indicateur du groupe dans l'association est mis égal au premier état avant d'évaluer les indicateurs des listes.

Une première association peut ainsi associer, en tant que membres, au moins un premier élément à un groupe dans l'une des deux listes, ou au moins un premier élément à un autre premier élément dans l'une des deux listes, ou au moins un groupe à un autre groupe dans l'une des deux listes.

En ce qui concerne les capacités, à chaque premier élément peut être associé un ensemble de couples d'indicateur d'autorisation et d'indicateur d'interdiction respectivement pour spécifier des droits d'accès du premier élément afin de n'autoriser et d'interdire des accès du premier élément à plusieurs actions relatives à un deuxième élément. Le procédé comprend alors les étapes de :

- dresser une liste de droits d'autorisation et d'interdiction et leur faire correspondre à chacun un couple d'indicateur d'autorisation et d'indicateur d'interdiction en les mettant respectivement aux premier et deuxième états pour une autorisation

d'accès et aux deuxième et premier états pour une interdiction d'accès, et

- n'autoriser le premier élément à un droit d'accès sur une action prédéterminée relative au deuxième élément que lorsque les indicateurs d'autorisation et d'interdiction pour ce droit d'accès sont respectivement aux premier et deuxième états, et n'interdire le droit d'accès à ladite action que lorsque les indicateurs d'autorisation et d'interdiction sont respectivement aux deuxième et premier états.

L'introduction de droit d'accès négatif dans les capacités selon l'invention permet de révoquer un droit d'accès pour un sujet donné, en donnant la possibilité de spécifier explicitement les interdictions d'accès d'un sujet. On garantit ainsi qu'un sujet donné ne peut acquérir la capacité lui permettant d'accéder à un objet déterminé. Plus précisément, une capacité négative permet de spécifier qu'un sujet donné ne peut acquérir le droit d'accès positif correspondant.

La capacité négative peut également être utilisée pour révoquer temporairement un droit d'accès. En particulier, conformément au principe du moindre privilège, selon lequel un sujet n'acquiert un droit d'accès que lorsqu'il a besoin de ce droit, il est judicieux de temporairement révoquer un droit d'accès d'un sujet, par exemple lorsque ce sujet acquiert par ailleurs un autre droit d'accès incompatible au regard de la sécurité du moyen de traitement de données.

Selon une autre caractéristique de l'invention, comme pour les listes de contrôle d'accès, l'incompatibilité entre les états des deux indicateurs du couple associé à un premier élément

est vérifié à chaque demande d'accès du premier élément à un deuxième élément. Lorsque les indicateurs d'autorisation et d'interdiction d'un couple sont tous deux au deuxième état, le droit d'accès peut être par défaut autorisé ou interdit ; une erreur de complétude peut être alors signalée. Lorsque les indicateurs d'autorisation et d'interdiction sont tous deux au premier état, le droit d'accès peut être par priorité autorisé ou interdit ; une erreur de consistance peut être alors signalée.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs réalisations préférées de l'invention en référence aux dessins annexés correspondants dans lesquels :

- la figure 1 est un diagramme montrant une matrice de contrôle d'accès entre trois sujets et quatre objets selon la technique antérieure ;
- la figure 2 est un algorithme d'étape principale d'un procédé de contrôle d'accès basé sur au moins une liste de contrôle d'accès selon l'invention ;
- la figure 3 est un algorithme d'authentification de sujet inclus dans le procédé selon la figure 2 ;
- la figure 4 est un algorithme de détermination de couple d'indicateur d'autorisation et d'indicateur d'interdiction associé à un sujet authentifié selon la figure 3 ; et
- la figure 5 est un algorithme de contrôle d'accès relatif à au moins une capacité d'accès selon l'invention.

En référence à la figure 2, un procédé basé sur des listes de contrôle d'accès ACL pour contrôler des accès de premiers éléments, tels que des sujets, à des deuxièmes éléments, tels que des objets dans un moyen de traitement de données, tel que le microcontrôleur d'une carte à puce, comprend principalement des étapes ET1 à ET5 en vue de déterminer un indicateur d'autorisation ou de droit positif pour autoriser un sujet déterminé à accéder à un objet donné, et complémentairement un indicateur d'interdiction ou de droit négatif pour interdire le sujet déterminé à accéder à l'objet. Par souci de simplification, on désigne par "accès" à l'objet donné, un droit permettant d'accomplir au moins une action sur l'objet donné.

A une première étape initiale ET1, un ensemble de sujet ES comprenant U sujets S1, ... Su, ...SU avec $1 \leq u \leq U$ est défini.

Selon l'invention, au concept sujet est également associé un concept de groupe de sujet selon lequel un groupe est autorisé à accéder à un objet dès que l'un des sujets inclus dans le groupe est autorisé à accéder à l'objet ; tous les droits accordés à un groupe sont accordés d'office à chaque élément appartement au groupe. L'étape ET1 définit également un ensemble EG de groupes G1, ... Gv, ... GV avec $1 \leq v \leq V$. Chaque groupe contient au moins deux sujets de l'ensemble ES, et plusieurs groupes peuvent avoir en commun des sujets.

Un sujet ou un groupe donné peut être associé à un autre sujet ou un autre groupe. L'étape ET1 définit également un ensemble EAS d'associations AS1,... ASw,... ASW avec $1 \leq w \leq W$. Une association ASw contient au moins deux membres, soit deux sujets

ou deux groupes, soit un sujet et un groupe. Un membre MEj d'une association ASw, qu'il soit sujet individuel ou sujet inclus dans au moins un groupe, est autorisé à accéder à un objet donnée Ob que lorsqu'à la fois tous les membres de l'association sont autorisés à accéder à l'objet donné.

Enfin l'étape ET1 définit un ensemble EO d'objets O1, ... Ob, ... OB avec $1 \leq b \leq B$. Des sujets prédéterminés peuvent demander d'accéder à chacun des objets à l'étape suivante.

L'étape suivante ET2 définit les conditions d'accès aux objets. A titre d'exemple, on se référera dans la suite à une liste de contrôle d'accès, c'est-à-dire aux conditions d'accès de sujets à un objet donné quelconque Ob de l'ensemble EO, les étapes ET2 à ET5 étant analogues quel que soit l'objet.

A l'étape ET2, deux listes A et I sont dressées, c'est-à-dire récupérées ou créées, et enregistrées dans le microcontrôleur. La première liste A contient des sujets autorisés individuellement Sm, des groupes autorisés de sujet Gn et des associations autorisées ASx qui sont autorisés à accéder à l'élément Ob, avec $1 \leq m \leq M \leq U$, $1 \leq n \leq N \leq V$ et $1 \leq x \leq X \leq W$. La deuxième liste dressée I contient des sujets interdits individuellement Sp, des groupes interdits de sujet Gq et des associations interdites ASy par lesquels l'accès au deuxième élément Ob est interdit, avec $1 \leq p \leq P \leq U$, $1 \leq q \leq Q \leq V$ et $1 \leq y \leq Y \leq W$. Ainsi, dans une liste A ou I, un sujet Sm ou Sp y est inclus à titre individuel, ou est inclus dans un groupe Gn ou Gq, ou bien encore est associé à un autre sujet ou à un groupe dans une association ASx ou ASy. L'appartenance d'un sujet ou d'un groupe donné à une association ASw implique que l'autorisation d'accès du sujet Su à l'objet Ob ne

peut être accordée que lorsque tous les membres ME1,... Mej,... MEj de l'association, y compris le sujet ou le groupe donné, sont authentifiés.

De manière plus générale, chacune des première et deuxième listes A et I contient au moins un sujet et/ou un groupe et/ou une association, chaque groupe contient au moins un sujet, et chaque association contient au moins deux membres.

Les étapes suivantes ET3, ET4 et ET5 sont des étapes itératives au cours d'une session avec la carte à puce. Au début d'une session, tous les indicateurs de sujet BSu, de groupe BGv et d'association BASw définis ci-après sont mis à zéro.

Les deux étapes principales ET3 et ET4 concernent ainsi au cours d'une session l'authentification d'un sujet quelconque Su demandant l'accès à l'objet donné Ob et la détermination des états d'un indicateur d'autorisation BA et d'un indicateur d'interdiction BI de manière à valider l'autorisation ou l'interdiction d'accès du sujet Su à l'objet Ob. Au cours du déroulement de ces deux étapes, les indicateurs des sujets, groupes et associations qui ont déjà été déterminés et qui ne sont pas relatifs au sujet Su demeurent inchangés.

La dernière étape ET5 marque la réitération pour un prochain sujet Su souhaitant accéder à l'objet Ob, quels que soient les résultats de l'authentification précédente et de la détermination précédente.

Dans la suite, un indicateur BSu d'un sujet Su, un indicateur BGv d'un groupe Gv, un indicateur de membre d'association BMEj, un indicateur d'association BASw et des indicateurs d'autorisation et d'interdiction BA et BI de l'objet Ob sont

supposés être des bits pouvant être à l'un de premier état binaire "1" et deuxième état binaire "0".

Un indicateur de groupe BGn ou BGq à l'état "0" signifie que tous les indicateurs des sujets inclus dans ce groupe sont à l'état "0", alors qu'un indicateur BGn ou BGq d'un groupe à l'état "1" signifie que l'indicateur d'au moins l'un des sujets appartenant à ce groupe est à l'état "1". L'indicateur d'une association BASw à l'état "0" signifie qu'au moins un indicateur BMEj d'un membre MEj de l'association est à l'état "0", alors qu'un indicateur BASw à l'état "1" signifie que tous les indicateurs des membres de l'association sont à l'état "1". Le concept de groupe correspond ainsi à l'opérateur OU logique, et le concept d'association correspond à l'opérateur ET logique.

En référence à la figure 3, l'étape principale d'authentification ET3 comprend des étapes ET31 à ET36.

La carte à puce procède à l'authentification proprement dite du sujet Su à l'étape suivante ET31. Par exemple, l'authentification consiste à reconnaître un mot de passe ou un code secret transmis par le sujet Su au microcontrôleur de la carte à puce qui le traite selon un algorithme d'authentification qui produit un résultat à comparer à des mots ou codes prémémorisés relatifs à des sujets inclus dans les listes A et I associées à l'objet Ob. Si le sujet Su n'est pas authentifié, le procédé passe à l'étape ET5. En revanche, si le sujet Su est authentifié, l'indicateur BSu est enregistré à l'état "1", à l'étape ET32.

Aux étapes suivantes ET33 et ET35, le procédé est dirigé vers l'étape de détermination ET4 si

l'élément Su n'appartient à aucun des groupes Gn ou Gq ou n'est membre d'aucune association ASx ou ASy.

Dans le premier cas contraire, si à l'étape ET33 le microcontrôleur de la carte à puce constate l'appartenance du sujet Su à au moins un groupe Gn ou Gq, les indicateurs BGn, BGq des groupes Gn, Gq auxquels appartient le sujet Su, ainsi que les indicateurs BMEj de ces groupes en tant que membres d'une association ASx ou ASy, sont mis à "1" à l'étape ET34, qui est suivie par l'étape de détection d'association ET35.

Si à l'étape ET35, le microcontrôleur de la carte à puce constate que le sujet Su est un membre d'une ou plusieurs associations ASx ou ASy, le microcontrôleur évalue à l'étape ET36 l'indicateur BASx ou BASy de chacune de ces associations égal au produit des indicateurs BEMj ou BEMk des membres MEj ou MEk de l'association :

$$BASx = \prod_{j=1}^{j=J} BEMj \; ; \; BASy = \prod_{k=1}^{k=K} BEMk$$

Dans ces relations, BMEj ou BEMk peut être l'indicateur BSu du sujet donné Su, ou l'indicateur BSm ou BSp d'un sujet-membre Sm dans la liste A ou Sp dans la liste I, ou encore l'indiateur BGn ou BGq d'un groupe-membre Gn dans la liste A ou Gq dans la liste I.

Comme après l'étape ET35, le procédé passe après l'étape ET36 à l'étape ET4.

Comme montré à la figure 4, l'étape de détermination ET4 débute par une étape ET40 pour évaluer et enregistrer l'indicateur d'autorisation BA et l'indicateur d'interdiction BI correspondant au

sujet Su relativement à l'accès à l'objet Ob, selon les relations binaires suivantes :

$$BA = \sum_{m=1}^{m=M} BSn + \sum_{n=1}^{n=N} BGn + \sum_{x=1}^{x=X} BASx$$

$$BI = \sum_{p=1}^{p=P} BSp + \sum_{q=1}^{q=Q} BGq + \sum_{y=1}^{y=Y} BASy$$

Dans les relations précédentes, les indicateurs relatifs au sujet Su, à des groupes incluant le sujet Su, et à des sujets et/ou groupes associés au sujet Su ont des états déterminés respectivement aux étapes ET34 et ET36.

Si le sujet Su appartient à plusieurs groupes et/ou est membre de plusieurs associations, plusieurs bits BGn et/ou BGq et/ou BASx et/ou BASy peuvent être à l'état "1".

Puis aux étapes suivantes, le couple (BA, BI) est analysé de manière à autoriser ou interdire l'accès du sujet Su à l'objet Ob et le cas échéant signaler des erreurs dans les listes de sujet A et I associées à l'objet Ob.

A l'étape ET41, le couple (BA, BI) est comparé au couple (1, 0). Si l'un des indicateurs d'autorisation BA est à l'état "1" et l'indicateur d'interdiction BI est à l'état "0", le microcontrôleur de la carte à puce autorise le sujet Su à accéder à l'objet Ob à l'étape ET42. En revanche, si après l'étape ET41, le bit d'autorisation BA est à l'état "0" et le bit d'interdiction BI est à l'état "1" à l'étape ET43, le microcontrôleur de la carte à puce interdit le sujet Su d'accéder à l'objet Ob à l'étape ET44.

Si après les étapes ET41 et ET43, le couple d'indicateurs (BA, BI) est différent des couples (1,

0) et (0, 1), c'est-à-dire si les indicateurs BA et BI sont au même état, le microcontrôleur de la carte à puce vérifie aux étapes suivantes ET45 et ET46 si le couple d'indicateurs (BA, BI) est égale à l'un des deux couples (0, 0) et (1, 1).

Si à l'étape ET45, les deux indicateurs d'état BA et BI sont à l'état "0", ceci signifie que les droits d'accès du sujet Su à l'objet Ob sont incomplets ; en d'autres termes, les droits d'accès de l'objet Ob n'offrent pas de complétude au sujet Su puisqu'un sujet ne peut pas à la fois ne pas être autorisé explicitement à accéder à l'objet Ob et ne pas être interdit explicitement à accéder à l'objet Ob. Cet état de non-complétude peut éventuellement être signalé par le microcontrôleur de la carte à puce sous la forme d'une erreur affichée sur l'écran d'un terminal accueillant la carte à puce, au développeur ou à la personne gérant les accès aux objets, à une étape ET49. Une règle par défaut, c'est-à-dire une autorisation d'accès par exemple, ou bien une interdiction d'accès du sujet Su à l'objet Ob s'applique.

Lorsque les indicateurs BA et BI sont tous deux à l'état "1" à l'étape ET46, ceci signifie que les listes des sujets A et I relatives à l'objet Ob sont inconsistantes, comme signalé à l'étape ET48. La consistance des listes A et I garantit que pour tout sujet et tout objet, si plusieurs droits d'accès d'un sujet à un objet sont définis, ils spécifient tous le même type de droit positif ou négatif. En d'autres termes, un sujet donné ne peut à la fois être autorisé à accéder à un objet donné et être interdit d'accès à cet objet. Une règle de priorité sélectionnant automatiquement l'un prédéterminé des droits d'autorisation et d'interdiction d'accès au

sujet Su sur l'objet Ob s'applique. Comme après l'étape ET47, l'étape ET48 peut être suivie par l'étape ET49 signalant une incohérence de la composition des listes A et I associées à l'objet Ob dans les listes A et I.

Finalement après l'étape ET42, ou ET44, ou ET49, le procédé passe à l'étape ET5.

Les exemples suivants illustrent divers chemins dans l'algorithme de procédé de contrôle d'accès montré aux figures 3 et 4.

Premier exemple :

Les ensembles

ES = {S0,S1,S2,S3,S4,S5,S6,S7,S8,S9,S10,S11,S12} et EG = {G1, G2} sont définis avec les conditions d'accès suivantes sur l'objet donné Ob aux étapes ET1 et ET2 :

A = {S1, S4, S6, G2},

I = {S5, S8, S9, G1},

avec G1 = {S2, S3, S10, S11},

et G2 = {S7, S12, S0}.

Selon un premier cas, le sujet S6 appartenant à la liste A demande à accéder à l'objet Ob. Après une authentification de l'objet S6 à l'étape ET3, soit BS6 = 1 et BS1 = BS4 = BG2 = BS5 = BS8 = BS9 = BG1 = 0, les indicateurs BA et BI sont déterminés à l'étape ET40 :

BA = BS1 + BS4 + BS6 + BG2 = 0 + 0 + 1 + 0 = 1

BI = BS5 + BS8 + BS9 + BG1 = 0 + 0 + 0 + 0 = 0

ce qui autorise l'accès du sujet S6 à l'objet Ob selon les étapes ET41 et ET42, puisque :

(BA, BI) = (1, 0).

Selon un deuxième cas, le sujet S8 appartenant à la liste I souhaite accéder à l'objet Ob. Après une

authentification du sujet S8, soit BS8 = 1 et BS1 = BS4 = BS6 = BG2 = BS5 = BS9 = BG1 = 0, les indicateurs BA et BI sont déterminés :

BA = BS1 + BS4 + BS6 + BG2 = 0 + 0 + 0 + 0 = 0

BI = BS5 + BS8 + BS9 + BG1 = 0 + 1 + 0 + 0 = 1,

ce qui interdit l'accès du sujet S8 à l'objet Ob selon les étapes ET43 et ET44, puisque :

(BA, BI) = (0, 1).

Selon un troisième cas, le sujet S7 appartenant au groupe G2 dans la liste A désire accéder à l'objet Ob. Après une authentification réussie du sujet S7, soit BS7 = BG2 = 1 et BS1 = BS4 = BS6 = BS5 = BS8 = BS9 = BG1 = 0, les indicateurs BA et BI de l'objet Ob sont déterminés :

BA = BS1 + BS4 + BS6 + BG2 = 0 + 0 + 0 + 1 = 1,

BI = BS5 + BS8 + BS9 + BG1 = 0 + 0 + 0 + 0 = 0,

ce qui autorise l'accès du sujet S7 inclus dans le groupe G2 à l'objet Ob, puisque :

(BA, BI) = (1, 0).

Deuxième exemple :

Les ensembles ES = {S1, S4, S5, S6, S7, S8, S9} et EG = {G1, G2} sont définis avec les conditions d'accès suivantes sur l'objet Ob, aux étapes ET1 et ET2 :

A = {S1, S4, S6, AS1},

I = {S5, S8, S9, G1},

avec G1 = {S3, S10, S11},

G2 = {S2, S12, S0}, et

AS1 = {G2, S7}.

Dans un premier cas de ce deuxième exemple, le sujet S7 est membre d'une association AS1 comprenant le groupe G2 et souhaite accéder à l'objet Ob, après une authentification préalable d'au moins l'un des éléments appartenant au groupe G2, ce qui impose BG2

= 1. Après une authentification réussie du sujet S7, les indicateurs d'éléments de groupes et d'association sont les suivants :

BG2 = BS7 = 1,

BAS1 = 1 x 1 = 1, et

BS1 = BS4 = BS6 = BS5 = BS8 = BS9 = BG1 = 0.

Les indicateurs d'autorisation et d'interdiction BA et BI sont ensuite évalués à l'étape ET40 :

BA = BS1 + BS4 + BS6 + BAS1 = 0 + 0 + 0 + 1 = 1

BI = BS5 + BS8 + BS9 + BG1 = 0 + 0 + 0 + 0 = 0.

Puisque le couple (BA, BI) est égal à (1, 0), le sujet S7 est autorisé à accéder à l'objet Ob.

Selon un deuxième cas du deuxième exemple, le sujet S7 associé au groupe G2 dans l'association AS1 souhaite encore accéder à l'objet Ob, mais aucun élément du groupe G2 n'a été préalablement authentifié, soit après l'étape d'authentification ET3 du sujet S7, les états suivants des indicateurs de sujets et de groupes :

BG2 = 0, BS7 = 1,

BAS1 = 0 x 1 = 0, et

BS1 = BS4 = BS6 = BS5 = BS8 = BS9 = BG1 = 0.

Les indicateurs d'autorisation et d'interdiction BA et BI sont ensuite évalués à l'étape ET40 :

BA = BS1 + BS4 + BS6 + BAS1 = 0 + 0 + 0 + 0 = 0,

BI = BS5 + BS8 + BS9 + BG1 = 0 + 0 + 0 + 0 = 0.

Les deux indicateurs BA et BI étant à l'état "0", une erreur de complétude est éventuellement signalée, la règle par défaut s'applique et l'accès du sujet S7 à l'objet Ob est interdit selon les étapes ET45 et ET47.

Troisième exemple :

L'ensemble de sujet ES = {S1, S4, S5, S6, S8, S9} et l'ensemble de groupe EG = {G1, G2} sont

définis avec les conditions d'accès suivantes sur l'objet Ob aux étapes ET1 et ET2 :

A = {S1, S4, S6, AS1},

I = {S5, S8, S9, G1},

avec G1 = {S3, S7, S10, S11},

G2 = {S2, S12, S1}, et

AS1 = {G2, S7}.

Dans cet exemple, le sujet S7 appartenant au groupe G1 a besoin d'accéder à l'objet Ob, et le groupe G2 associé au sujet S7 dans l'association AS1 a été préalablement authentifié, par exemple par authentification préalable du sujet S2, soit BS2 = BG2 = 1. Après authentification du sujet S7, les indicateurs de sujets et de groupes sont les suivants :

BS2 = BG2 = BS7 = BG1 = 1,

BAS1 = 1 x 1 = 1, et

BS1 = BS4 = BS6 = BS5 = BS8 = BS9 = 0.

Les indicateurs d'autorisation et d'interdiction sont ensuite évalués à l'étape ET40 :

BA = BS1 + BS4 + BS6 + BAS1 = 0 + 0 + 0 + 1 = 1

BI = BS5 + BS8 + BS9 + BG1 = 0 + 0 + 0 + 1 = 1.

La règle de priorité s'applique puisqu'il y a une inconsistance résultant de l'état du couple (BA, BI) = (1, 1) selon les étapes ET46 et ET48. Si la règle de priorité est par exemple négative, alors l'accès du sujet S7 à l'objet Ob est interdit.

Quatrième exemple :

L'ensemble de sujet ES = {S1, S4, S5, S6, S8, S9} et l'ensemble de groupe EG = {G1, G2} sont définis avec les conditions d'accès suivantes sur l'objet Ob :

A = {S1, S4, S6, AS1},

I = {S5, S8, S9, G1, S1},

avec G1 = {S3, S7, S10, S11},

G2 = {S2, S12}, et

AS1 = {G2, S7}.

Si le sujet S1 souhaite accéder à l'objet Ob, le sujet S1 est d'abord authentifié à l'étape ET3, soit :

BS1 = 1 et BS4 = BS6 = BG2 = BS7 = BAS1 = BS5 = BS8 = BS9 = BG1 = 0.

Les indicateurs BA et BI sont évalués à l'étape ET40 :

BA = BS1 + BS4 + BS6 + BAS1

= 1 + 0 + 0 + 0 x 0 = 1,

BI = BS5 + BS8 + BS9 + BG1 + BS1

= 0 + 0 + 0 + 0 + 1 = 1.

Là encore une inconsistance peut éventuellement être signalée et la règle de priorité s'applique à l'étape ET48. Le sujet S1 n'a pas accès à l'objet Ob puisque les deux indicateurs BA et BI sont à l'état "1" à l'étape ET46.

Selon une deuxième réalisation, le procédé de contrôle d'accès concerne au moins une capacité d'accès d'un sujet donné Su sur au moins un objet Ob. La capacité du sujet Su est définie par une référence de l'objet, telle que son nom, et par un ensemble de privilèges ou de droits qui définissent des actions pouvant être ou ne pouvant pas être accomplies par le sujet sur l'objet. Pour introduire des droits négatifs, à chaque droit positif correspond la négation de ce droit positif. En d'autres termes, à une autorisation en lecture correspond une interdiction en lecture, à une autorisation d'exécution correspond une interdiction d'exécution, etc.

En référence à la figure 5, le procédé de contrôle d'accès relatif à une capacité du sujet Su sur l'objet Ob comporte des étapes ET2a à ET5a. Au cours d'une étape préliminaire ET2a, un ensemble de droits positifs et négatifs {D1, ... Dk, ... DK} sont définis par correspondance à chacun des droits, tels que écriture, exécution, lecture, etc..., d'un couple d'indicateurs d'autorisation et d'interdiction (BAk, BIk). Si le droit est positif, l'indicateur d'autorisation BAk est enregistré à un premier état logique "1" et l'indicateur d'interdiction BIk est enregistré à l'état logique "0". En revanche si le droit est négatif, par exemple si le sujet Su n'est pas autorisé à accéder à une lecture du programme Ob, l'indicateur d'autorisation BAk est enregistré au deuxième état logique "0" et l'indicateur d'interdiction BIk est enregistré au premier état logique "1".

Puis une étape ET31a analogue à l'étape ET31 (figure 3) est exécutée au cours de laquelle le sujet Su est authentifié par le microcontrôleur de la carte à puce, de manière à procéder à la détermination de la capacité (BAk, BIk) du sujet Su liée au droit Dk dans l'objet Ob à partir de l'étape ET50.

Si à l'étape suivante ET51 les indicateurs BAk et BIk sont respectivement égaux à "1" et "0", l'étape ET52 donne l'accès du sujet Su au droit Dk dans l'objet Ob, c'est-à-dire l'autorisation d'exécuter l'action Dk sur l'objet Ob. Par contre, si les indicateurs BAk et BIk sont respectivement égaux à "0" et "1" à l'étape ET53, le droit Dk est refusé au sujet Su à l'étape ET54.

D'une manière analogue aux étapes ET45 à ET49, des étapes ET55 à ET59 détectent une erreur dans la liste des droits d'accès par le sujet Su à l'objet

Ob. Si à l'étape ET55 les deux indicateurs BAk et BIk sont à l'état "0", l'étape ET57 détecte qu'il n'y a pas de complétude dans la liste des droits d'accès et le microcontrôleur applique une règle par défaut, c'est-à-dire soit l'autorisation, soit l'interdiction du droit D et détecte une erreur à l'étape ET59. Si à l'étape ET56, les indicateurs BAk et BIk sont tous deux à l'état "1", la liste des droits d'accès est inconsistante à l'étape ET58 ; le microcontrôleur applique une règle de priorité en sélectionnant l'une prédéterminée des autorisation et interdiction du droit Dk et détecte une erreur à l'étape ET59.

Après les étapes ET52, ET54 et ET59, le procédé réitère à une étape ET5a les étapes précédentes pour la capacité d'un autre sujet ou la capacité du sujet Su pour un objet autre que l'objet Ob.

Ainsi pour définir des droits positifs selon la technique antérieure, ainsi que des droits négatifs, l'invention associe à chaque droit un indicateur d'autorisation ou d'interdiction de ce droit et un indicateur contraire à ce droit et vérifie la complétude et la consistance de chaque couple d'indicateurs relatif à une action positive ou négative déterminée, telle que écriture, lecture, exécution, sauvegarde, enregistrement autorisé ou interdit.

Selon une réalisation plus complète, les figures 2, 3 et 4 sont combinées avec la figure 5, c'est-à-dire les étapes ET2 et ET31 sont combinées respectivement avec les étapes ET2a et ET31a, et les étapes ET50 à ET59 succèdent à l'étape ET42 afin d'autoriser l'accès d'un sujet authentifié Su à des droits Dk relatifs à un objet Ob lorsque le couple d'indicateurs d'autorisation d'interdiction (BA, BI)

est égal à (1, 0) et les couples d'indicateurs de droit (BAk, BIk) sont égaux à (1, 0).

A titre d'exemple, cinq droits d'accès sont prévus pour un objet Ob, tel qu'une application. Ces droits sont la lecture/non-lecture, l'écriture/non-écriture, exécution/non-exécution, sauvegarde/non-sauvegarde, enregistrement/non-enregistrement.

Il est supposé qu'un sujet Su présente la capacité suivante à l'étape ET2a :

{BA1, ..., BAK ; BIA, ..., BIK} = {1, 0, 1, 0, 0 ; 0, 1, 0, 1, 1}

ce qui signifie que le sujet Su est seulement autorisé à accéder en lecture et en exécution à l'objet Ob puisque BA1 = BA3 = "1" et qu'il lui est interdit d'accéder en écriture, sauvegarde et enregistrement à l'objet Ob puisque BI2 = BI4 = BI5 = 1.

Par exemple si le sujet Su souhaite accéder à une lecture de l'objet Ob à l'étape E31a, le microcontrôleur de la carte à puce constate à l'étape ET51 que le couple d'indicateurs (BA1, BI1) est égal à (1, 0) de manière à autoriser à l'étape ET52 la lecture de l'objet Ob par le sujet Su. Par contre, si à une étape suivante ET31a le sujet Su demande un accès en écriture de l'objet Ob, le microcontrôleur refuse cet accès à l'étape ET54 puisqu'il constate que le couple d'indicateurs (BA2, BI2) est égal à (0, 1) à l'étape ET53.

REVENDICATIONS

1 - Procédé pour contrôler des accès de premiers éléments (Su) à des deuxièmes éléments (Ob) dans un moyen de traitement de données, caractérisé par un enregistrement (ET40) dans le moyen de traitement d'indicateurs d'autorisation (BAk) ayant chacun un premier état pour autoriser explicitement un accès au moins d'un premier élément (Su) à un deuxième élément (Ob) et un deuxième état pour ne pas autoriser ledit accès, et d'indicateurs d'interdiction (BIk) ayant chacun le premier état pour interdire explicitement un accès au moins d'un premier élément à un deuxième élément et le deuxième état pour ne pas interdire ledit accès, l'accès étant autorisé ou interdit après une analyse (ET4) conjointe des indicateurs d'autorisation et d'interdiction relatifs à l'accès par le moyen de traitement de données.

2 - Procédé conforme à la revendication 1, caractérisé en ce que, pour donner l'accès d'un premier élément (Su) parmi plusieurs éléments d'un ensemble (ES) à un deuxième élément (Ob), il comprend les étapes de :

- dresser (ET2) une première liste (A) de premiers éléments (Sm) auquel l'accès au deuxième élément (Ob) est autorisé et une deuxième liste (I) de premiers éléments (Sp) auquel l'accès aux deuxièmes éléments est interdit,
- mettre (ET32) respectivement au premier état l'indicateur (BSu) d'un premier élément des première et deuxième listes lorsque le premier élément est authentifié et au deuxième état lorsque le premier élément n'est pas authentifié,
- évaluer (ET40) un indicateur d'autorisation (BA) en fonction des indicateurs (BSm) des éléments

dans la première liste et un indicateur d'interdiction (BI) en fonction des indicateurs (BSp) des éléments dans la deuxième liste, et

- n'autoriser (ET41, ET42) l'accès du premier élément (Su) au deuxième élément (Ob) que lorsque les indicateurs d'autorisation et d'interdiction (BA, BI) sont respectivement au premier état et au deuxième état, et n'interdire (ET43, ET44) l'accès du premier élément au deuxième élément que lorsque les indicateurs d'autorisation et d'interdiction sont respectivement au deuxième état et au premier état.

3 - Procédé conforme à la revendication 2, selon lequel lorsque les indicateurs d'autorisation et d'interdiction sont tous deux au deuxième état (ET45, ET47), l'accès est par défaut autorisé ou interdit.

4 - Procédé conforme à la revendication 2 ou 3, selon lequel lorsque les indicateurs d'autorisation et d'interdiction (BA, BI) sont tous deux au premier état (ET46, ET48), l'accès est par priorité autorisé ou interdit.

5 - Procédé conforme à l'une quelconque des revendications 2 à 4, selon lequel les première et deuxième listes (A, I) comprennent des groupes de premier élément (Gn, Gq) auxquels des indicateurs de groupe (BGn, BGq) correspondent pour autoriser ou interdire l'accès du groupe au deuxième élément (Ob), chaque groupe est considéré comme authentifié lorsque l'un des éléments du groupe est authentifié, et l'indicateur (BGn, BGq) d'un groupe contenant un élément authentifié est mis (ET34) au premier état avant d'évaluer (ET40) les indicateurs des listes.

6 - Procédé conforme à l'une quelconque des revendications 2 à 5, selon lequel les première et deuxième listes (A, I) comprennent des associations de premier élément (ASx, ASy) auxquelles des indicateurs d'association (BASx, BASy) correspondent pour autoriser ou interdire l'accès de l'association au deuxième élément (Ob), chaque association est considérée comme authentifiée lorsque tous les membres (BEMj, BEMk) de l'association sont authentifiés, et l'indicateur (BASx, BASy) d'une association contenant un élément authentifié est mis (ET34) égal au produit des indicateurs (BEMj, BEMk) des membres de l'association avant d'évaluer (ET40) les indicateurs des listes.

7 - Procédé conforme à la revendication 6, selon lequel au moins un membre (MEj, MEk) dans une association (ASx, ASy) dans l'une des deux listes (A, I) est un groupe (Gn, Gq), et, lorsque l'un des éléments du groupe est authentifié, l'indicateur (BGn, BGq) du groupe dans l'association est mis (ET34) égal au premier état avant d'évaluer (ET40) les indicateurs des listes.

8 - Procédé conforme à l'une quelconque des revendications 1 à 7, caractérisé en ce que, pour donner des droits d'accès d'un premier élément (Su) à plusieurs actions relatives à un deuxième élément (Ob), il comprend les étapes de :

- dresser (ET2a) une liste de droits d'autorisation et d'interdiction et leur faire correspondre à chacun un couple d'indicateur d'autorisation et d'indicateur d'interdiction (BAk, BIk) en les mettant respectivement aux premier et deuxième états pour une autorisation d'accès et aux

deuxième et premier états pour une interdiction d'accès, et

- n'autoriser le premier élément (Su) à un droit d'accès sur une action prédéterminée relative au deuxième élément (Ob) que lorsque les indicateurs d'autorisation et d'interdiction (BAk, BIk) pour ce droit d'accès sont respectivement aux premier et deuxième états, et n'interdire le droit d'accès à ladite action que lorsque les indicateurs d'autorisation et d'interdiction sont respectivement aux deuxième et premier états.

9 - Procédé conforme à la revendication 8, selon lequel lorsque les indicateurs d'autorisation et d'interdiction d'un couple sont tous deux au deuxième état (ET55, ET57), le droit d'accès est par défaut autorisé ou interdit.

10 - Procédé conforme à la revendication 8 ou 9, selon lequel lorsque les indicateurs d'autorisation et d'interdiction (BA, BI) sont tous deux au premier état (ET56, ET58), le droit d'accès est par priorité autorisé ou interdit.

Fig. 1

objet / sujet	F1	F2	F3	P1
S1	enregistre lecture écriture			exécution
S2		lecture	lecture écriture	enregistre lecture écriture exécute
S3	enregistre lecture	lecture écriture		lecture exécution

MA

capacité

ACL

Fig. 2

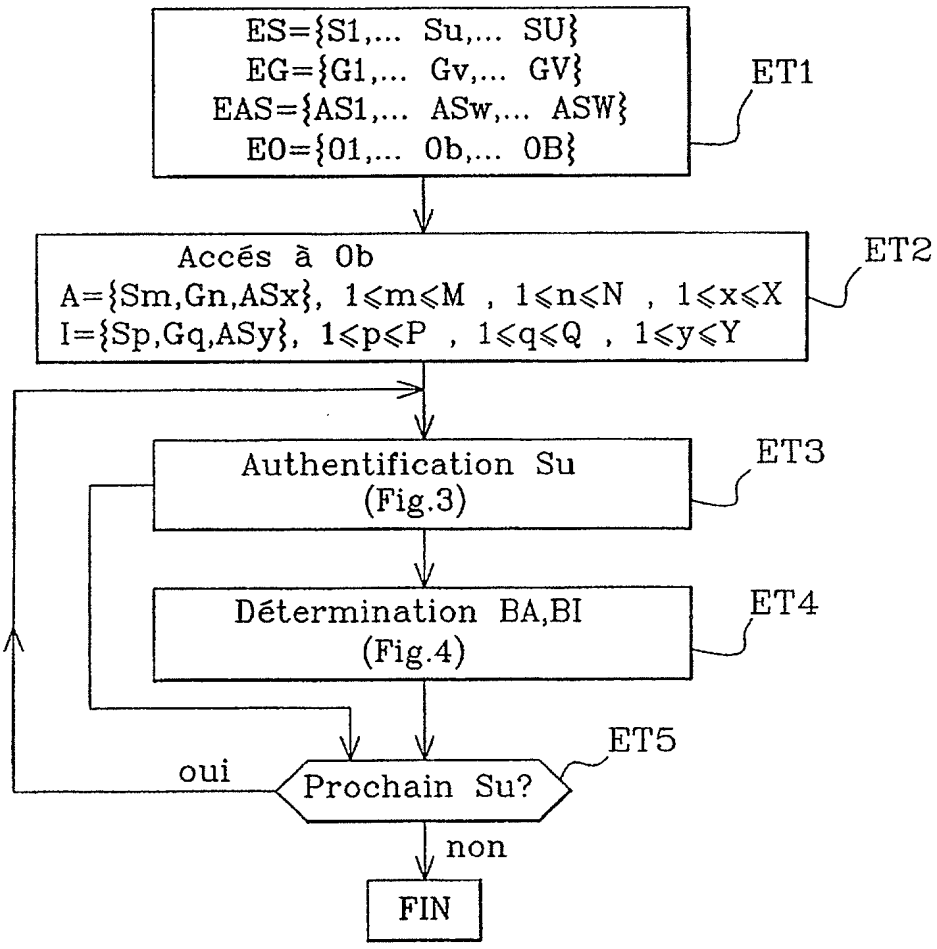
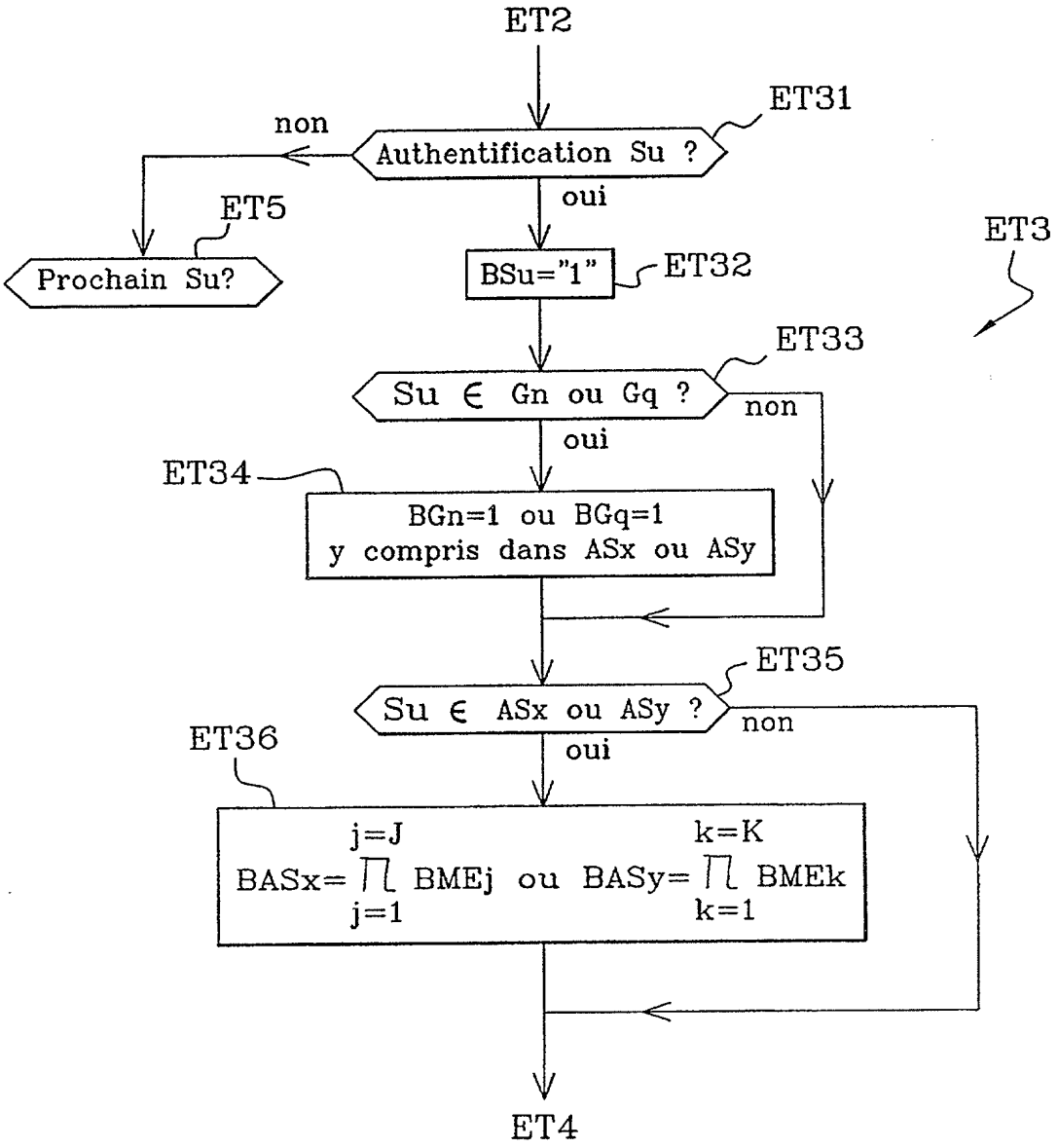


Fig. 3


ET2
ET31
non
Authentification Su ?
oui
ET5
Prochain Su?
ET3
BSu="1"
ET32
ET33
Su ∈ Gn ou Gq ?
non
oui
ET34
BGn=1 ou BGq=1
y compris dans ASx ou ASy
ET35
Su ∈ ASx ou ASy ?
non
oui
ET36
BASx= ∏ BMEj ou BASy= ∏ BMEk
j=1 j=J
k=1 k=K
ET4

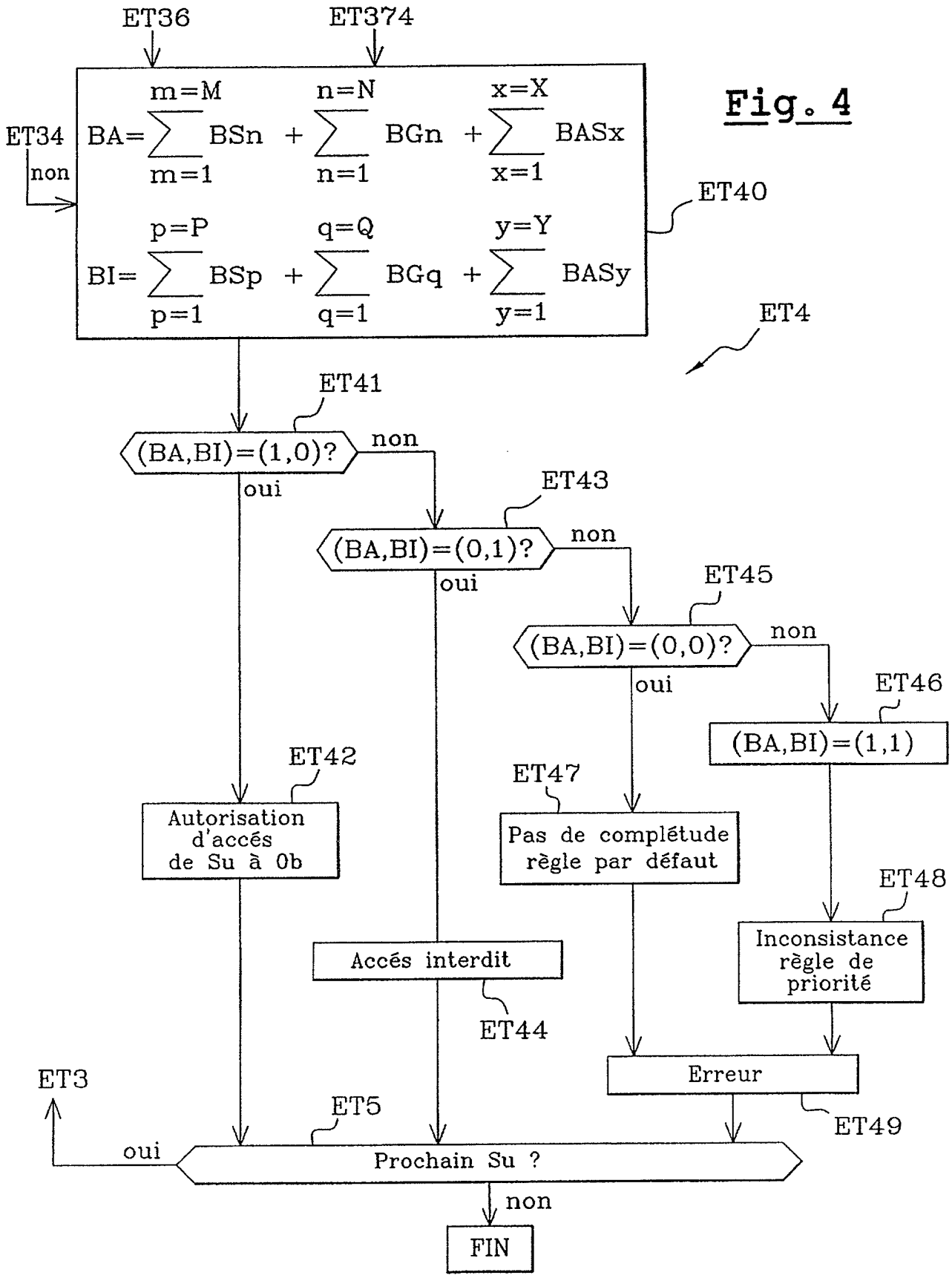

ET36
ET374
ET34
non
$BA=\sum_{m=1}^{m=M} BSn + \sum_{n=1}^{n=N} BGn + \sum_{x=1}^{x=X} BASx$
$BI=\sum_{p=1}^{p=P} BSp + \sum_{q=1}^{q=Q} BGq + \sum_{y=1}^{y=Y} BASy$
ET40
ET4
ET41
(BA,BI)=(1,0)?
non
oui
ET43
(BA,BI)=(0,1)?
non
oui
ET45
(BA,BI)=(0,0)?
non
oui
ET46
(BA,BI)=(1,1)
ET42
Autorisation d'accés de Su à 0b
ET47
Pas de complétude règle par défaut
ET48
Inconsistance règle de priorité
Accés interdit
ET44
Erreur
ET49
ET3
ET5
oui
Prochain Su ?
non
FIN

Fig. 4

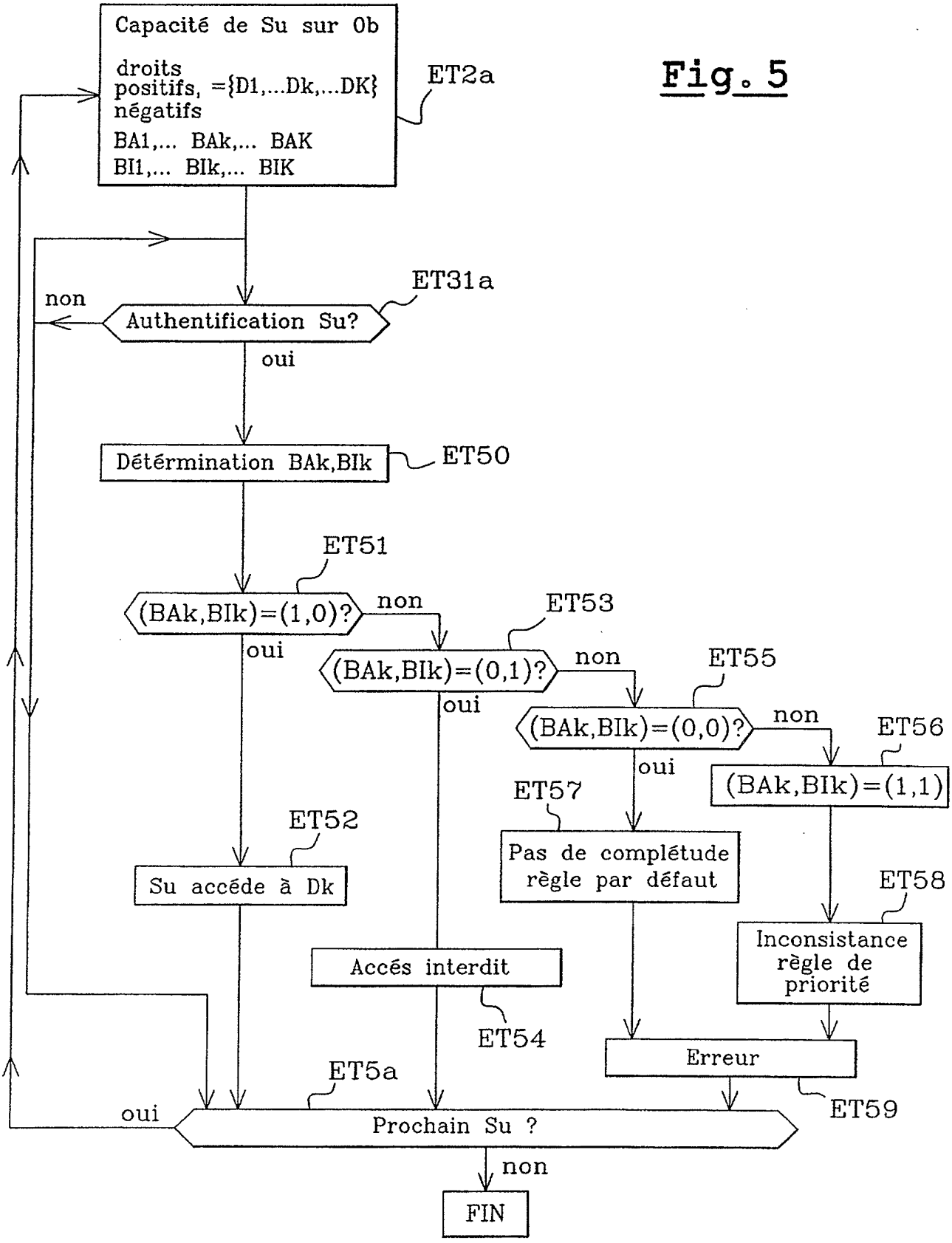

Capacité de Su sur Ob
droits positifs, négatifs
={D1,...Dk,...DK}
BA1,... BAk,... BAK
BI1,... BIk,... BIK
ET2a
ET31a
non
Authentification Su?
oui
Détérmination BAk,BIk
ET50
ET51
(BAk,BIk)=(1,0)?
non
oui
ET53
(BAk,BIk)=(0,1)?
non
oui
ET55
(BAk,BIk)=(0,0)?
non
oui
ET56
(BAk,BIk)=(1,1)
ET57
Pas de complétude règle par défaut
ET52
Su accéde à Dk
ET58
Inconsistance règle de priorité
Accés interdit
ET54
Erreur
ET59
ET5a
oui
Prochain Su ?
non
FIN

Fig. 5

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2820847

N° d'enregistrement national

FA 600397
FR 0101901

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	EP 0 913 966 A (SUN MICROSYSTEMS INC) 6 mai 1999 (1999-05-06)	1	G06F12/14
A	* colonne 11, ligne 42 - colonne 12, ligne 17 * * colonne 14, ligne 35 - ligne 42 * * figures 3-5 *	2-5,8-10	
X	WO 99 64948 A (MICROSOFT CORP) 16 décembre 1999 (1999-12-16)	1	
A	* page 8, ligne 30 - page 10, ligne 4 * * page 11, ligne 1 - ligne 18 * * figures 1-3 *	2,5,8	

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

G06F

1

Date d'achèvement de la recherche	Examinateur
29 octobre 2001	Arbutina, L

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0101901 FA 600397

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 29-10-2001
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0913966 A	06-05-1999	US 6064656 A	16-05-2000
		EP 0913966 A2	06-05-1999
		JP 11338839 A	10-12-1999
WO 9964948 A	16-12-1999	US 6279111 B1	21-08-2001
		EP 1084464 A1	21-03-2001
		WO 9964948 A1	16-12-1999

EPO FORM P0465